

Ex Parte

HUAWEI TECHNOLOGIES USA
875 15th Street, NW
Suite 825
Washington, DC 20005
www.usahuawei.com



May 16, 2013

Mr. Marlene Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington DC 20554

Re: IB Docket No. 12-343; Sprint Nextel Corp. and SoftBank Corp., Joint Application for
Consent to Transfer International and Domestic Authority

Dear Ms. Dortch:

Huawei Technologies USA (“Huawei”) submits this letter in the above referenced proceeding to inform the Commission’s public interest evaluation of the proposed transaction solely as it relates to the telecommunications network equipment of our company.¹ Huawei is aware of reports indicating that, to allay concerns with regard to U.S. national security, assurances or commitment were obtained from the Applicants to not integrate Huawei equipment into, and to take steps to remove Huawei equipment from, the wireless telecommunications networks relevant to the proposed transaction.² If the Commission were to condition approval of the Joint Application on any such assurance or commitment, Huawei believes it would ignore the experience of the more than 600 operators in over 150 countries worldwide that have deployed our equipment without incident, reflecting Huawei’s commitment to, and its record on, the security assurance of our products and our customers’ networks. In addition, it would unjustly limit the Applicants’ choice of suppliers, thereby restraining the competitive market benefits that would otherwise accrue to the Applicants and their customers. Huawei submits that neither the record in this proceeding nor any other evidence justify a condition that codifies any such

¹ Huawei recognizes that, “[T]he Commission takes into account the record developed in each particular case and accords deference to Executive branch agencies on issues related to national security, law enforcement, foreign policy, and trade policy.” *Review of Foreign Ownership Policies for Common Carrier and Aeronautical Radio Licensees Under Section 310(b)(4) of the Communications Act of 1934, as Amended* (“Review of Foreign Ownership Policies”), IB Docket No. 11-133, Second Report and Order, at 11 ¶ 13 (April 18, 2013). *See also Market Entry and Regulation of Foreign-Affiliated Entities*, IB Docket No. 95-22, Report and Order, 11 FCC Rcd 3897 ¶ 62 (1996). Through this letter, Huawei seeks to bring the matter to the attention of the FCC and the relevant Executive branch agencies.

² *See* “Chairman Rogers Statement on Proposed SoftBank/Sprint Deal: SoftBank/Sprint Plans Will Not Integrate Huawei Equipment,” H. Permanent Select Comm. on Intelligence (March 28, 2013), <http://intelligence.house.gov/press-release/chairman-rogers-statement-proposed-softbanksprint-deal>; *SoftBank slams Dish’s Sprint bid, rules out sweeteners*, REUTERS, April 30, 2013, <http://www.reuters.com/article/2013/04/30/us-softbank-sprint-idUSBRE93T05L20130430>; *Sprint bids: Dish’s Ergen swings back at Softbank’s Son*, USA TODAY, May 2, 2013, <http://www.usatoday.com/story/tech/2013/05/01/ergen-interview/2127487/>, and Spencer C. Ante, *SoftBank CEO Touts Proposed Sprint Take Over*, WALL ST. J., May 9, 2013.

assurance or commitment. Huawei urges the Commission to consider the facts on this matter, as set forth in more detail below, in its public interest evaluation of the proposed transaction.

As a multi-national corporation with its headquarters located in China,³ Huawei recognizes that “it needs to be committed to going the extra mile in cyber security assurance.”⁴ That is why Huawei is committed to “never stop in our endeavors to ensure that the greatest level of risk mitigation is applied to our products and their customers.”⁵ In sworn Congressional testimony, Huawei affirmed that it, “has not and will not jeopardize our global commercial success nor the integrity of our customers’ networks for any third party, government or otherwise. Ever.”⁶ To do so, Huawei recognizes, “would blemish our reputation, would have an adverse effect in the global market, and ultimately would strike a fatal blow to the company’s business operations.”⁷

Huawei has established and implemented an end-to-end, global cyber security assurance system that continuously incorporates cyber security elements into our core business processes, such as research and development, supply chain, service delivery, and supplier management.⁸ In several countries, including the United States, Huawei also engages third party testing organizations to conduct independent security audits and certifications on Huawei products.⁹ What we learn from these audits informs all of our processes, standards and policies, and is applied to all products and services in a virtual cycle.¹⁰

Huawei believes that cyber security is not a single country or a specific company issue.¹¹ The fact is that the information and communications technology (ICT) sector is comprised of a global, interdependent ecosystem in which “equipment and software are likely to be designed, developed and manufactured via tens, if not hundreds, of companies from around the world.”¹²

³ Huawei Technologies is a leading global information and communications technology (ICT) solutions provider. Through our dedication to consumer-centric innovation and strong partnerships, we have established end-to-end advantages in telecommunications networks, devices, and cloud computing. Huawei is committed to creating maximum value for our customers by providing competitive solutions and services. The company’s products and solutions have been deployed in over 150 countries, serving more than one-third of the world’s population.

⁴ John Suffolk, *Cyber Security Perspectives: 21st Century Technology and Security—a Difficult Marriage*, at 12 (Sept. 2012) (“Huawei white paper”), available at <http://www.huawei.com/en/about-huawei/corporate-info/CyberSecurity/index.htm>.

⁵ Annual Report 2012, Huawei Technologies, Co., Ltd., at 28 (April 2013), <http://www.huawei.com/en/about-huawei/corporate-info/annual-report/annual-report-2012/index.htm>.

⁶ *Hearing on Threat Posed by Chinese Telecommunications Companies: Hearing Before the H. Permanent Select Comm. on Intelligence*, 112th Cong. 6 (2012) (statement of Charles Ding, Corporate Vice President of Huawei).

⁷ *Id.*

⁸ Annual Report 2012, at 28-29.

⁹ *Id.* at 29.

¹⁰ Suffolk, at 15. As stated in the Huawei white paper, Huawei allows our processes and internal systems to be opened up to audit and scrutiny by customers and governments – that is, “to inspect, vet and validate our approach” – which enables Huawei to develop world-class processes and integrated systems. *Id.*

¹¹ Suffolk at 3.

¹² *Id.* at 10. See also U.S. GOV’T ACCOUNTABILITY OFFICE, IT SUPPLY CHAIN: NATIONAL SECURITY-RELATED AGENCIES NEED TO BETTER ADDRESS RISKS (2012), <http://www.gao.gov/assets/590/589568.pdf>. The report affirms that commercial information technology providers rely on a global supply chain to “design, develop, manufacture, and distribute hardware and software products throughout the world.” The report adds, “Many of the manufacturing

Moreover, company reports of every major telecommunications equipment provider reveal that each has a substantial base in China.¹³ The fact that approximately one-third of Huawei's components are sourced from U.S.-based software, hardware, and service suppliers should arouse no greater security concerns by a foreign government than should U.S. Government concerns be aroused by the geographic location of Huawei's (or any other equipment provider's) suppliers, assembly facilities, warehouses, or headquarters. Given this paradigm, Huawei's model for assessing risk is based on the philosophy, "we assume nothing, we believe no one, and we check everything."¹⁴

This precise viewpoint was recently expressed by 11 U.S. technology and business trade associations in a letter to leaders of the U.S. Congress on a restrictive provision in appropriations legislation related to procurement of information technology (IT) systems.¹⁵ The letter states,

"Fundamentally, **product security is a function of how a product is made, used, and maintained, not by whom or where it is made.** Geographic-based restrictions run the risk of creating a false sense of security when it comes to advancing our national cybersecurity interests. As a time when greater global cooperation and collaboration is essential to improve cybersecurity, geographic-based restrictions in any form risk undermining the advancement of global best practices and standards of cyber security."¹⁶ (emphasis added)

Similarly, a white paper released last month by the Brookings Institution entitled, *Building Trust in the Global Supply Chain*,¹⁷ maintains that because the ICT supply chain is global, "[p]articularistic solutions aimed at one part of the ecosystem are not going to be successful."¹⁸

inputs required for those products—whether physical materials or knowledge—are acquired from various sources around the global." *Id.* at 4.

¹³ Suffolk at 9 -10. "Cisco has a huge presence in China, with R&D centres in six major cities. Over 25 percent of all Cisco products are produced by Chinese partners.... Alcatel-Lucent has one-third of its global manufacturing done by Shanghai Bell; Ericsson's joint venture Nanjing Ericsson Panda Communications Co. has become the largest supply centre of Ericsson in the world; at the end of 2011, Nokia Siemens Networks had 10 manufacturing facilities worldwide: 5 in China..." (citations omitted) *Id.*

¹⁴ *Id.* at 8.

¹⁵ See Letter to The Honorable John Boehner, Speaker of the House, The Honorable Nancy Pelosi, The Honorable Harry Reid, and The Honorable Mitch McConnell, on Section 516 of the Consolidated and Further Continuing Appropriations Act for Fiscal Year 2013, P.L. 113-6 (April 4, 2013) ("Letter to Congressional Leaders"), signed by BSA | the Software Alliance, Emergency Committee for American Trade, Information Technology Industry Council, Semiconductor Industry Association, Software & Information Industry Association, TechAmerica, Technology CEO Council, Telecommunications Industry Association, U.S. Chamber of Commerce, U.S. Council for International Business, U.S. Information Technology Office, <http://www.techamerica.org/techamerica-leads-industry-opposition-to-onerous-provision-in-cr-that-hurts-u-s-tech-companies/>. See also Letter to The Honorable Harry Reid, The Honorable John Boehner, The Honorable Mitch McConnell, The Honorable Nancy Pelosi, from John Frisbie, President, U.S. China Business Council (April 8, 2013), <https://www.uschina.org/files/public/documents/2013/04/letter-cybersecurity.pdf>.

¹⁶ Letter to Congressional Leaders.

¹⁷ Darrell M. West, *Twelve Ways to Build Trust in the ICT Global Supply Chain*, The Brookings Inst., at 2 (April 2013).

¹⁸ *Id.*

Rather, the paper calls for “universal, comprehensive and standardized solutions... that involve product evaluation and reliance on trusted delivery systems.”¹⁹

Consistent with this view, Huawei believes that cyber security is a shared global challenge that is not limited to a particular geographic region, culture, language or technology provider. Huawei also believes that blocking an operator’s commercial agreements with one supplier will not result in any heightened degree of security; at most, it will generate a greater “sense” of security that plainly has no rational basis.

Huawei is aware that one filing in this proceeding raises the notion that Huawei’s network equipment would pose a risk to U.S. national security.²⁰ However, the filing relies entirely on a Congressional report that itself proffers no credible, factual evidence to substantiate its findings.²¹ The assertions made in that report are largely premised on perceptions that the extensive information and documentation Huawei made available during the course of the Congressional investigation did not disprove allegations made by others. And Huawei was not alone in its assessment of that report.²²

In addition to security-related concerns, limiting the Applicants’ choice of network equipment suppliers will result in less competition and the recognized benefits of a competitive equipment market. As noted in the FCC’s National Broadband Plan, “Competition is crucial for promoting consumer welfare and spurring innovation and investment in broadband access networks. Competition provides consumers the benefits of choice, better service and lower prices.”²³ More directly, the Commission notes in its most recent Mobile Competition Report, “A high level of network deployment costs (a type of fixed cost of building network capacity) in relation to the number of customers may limit the number of firms that can enter and survive in a market.”²⁴ If, indeed, one role of competition is to “determine whether there are any relevant regulatory policy tools that can reduce entry delay,”²⁵ imposing a limitation on competition in the network equipment market will have the opposite effect: it will likely increase entry delay, reduce the speed of or defer network upgrades, and result in higher prices for consumers and a lower level of mobile service adoption.

¹⁹ *Id.*

²⁰ See Petition to Deny or Impose Conditions, Communications Workers of America, at 14 (Jan. 28, 2013).

²¹ *Id.* See also INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE, A REPORT BY CHAIRMAN MIKE ROGERS AND RANKING MEMBER, C.A. DUTCH RUPPERSBERGER OF THE PERMANENT SELECT COMMITTEE ON INTELLIGENCE (Oct. 8, 2012) at 1, 7.

²² *Editorial: House Report on Huawei Shows Lack of Trust in China*, WASH. POST, Aug. 24, 2012, stating, “[T]he committee’s unclassified report falls short,” and “offers no evidence of ‘bugs, beacons, and backdoors.’” Further, the Post said, “if there is a real threat, such an alarm would be a lot more credible with some evidence.” *Id.* See also *Put on Hold: Two big Chinese telecoms firms come under fire in America*, THE ECONOMIST, Oct. 31, 2012, <http://www.economist.com/node/21564585>, saying the report “appears to have been written for vegetarians. At least there is not much meat in it” and “it presents little hard evidence to support its recommendations.” *Id.*

²³ FED. COMM’NS COMM., CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 26 (March 17, 2010).

²⁴ Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, *Sixteenth Report*, WT Docket 11-186, at 67-68 ¶ 79 (Mar. 21, 2013).

²⁵ *Id.*

A feature article in an August 2012 edition of The Economist argues that, “banning Huawei from bidding for commercial contracts is wrongheaded, for two reasons.”²⁶ The first reason, the article contends, is that competition from China generates economic benefits, and competition from Huawei, “is huge,” helping to “boost growth and thus wellbeing.”²⁷ Second is “the dirty little secret that its foreign rivals strangely neglect to mention: just about everybody makes telecoms equipment in China these days.”²⁸ The article concludes, “The answer is to insist on greater scrutiny all around, not just of Chinese firms. Governments should be crystal clear about what conditions telecoms firms need to meet to win business... [and] do more to ensure that equipment is secure, no matter who makes it.”²⁹

Thus, given Huawei’s commitment, undertakings, and record on the security of our products and our customers’ networks, and the absence of any factual evidence in the record or elsewhere to substantiate any claim that Huawei’s equipment poses a national security threat, it would be wholly unjustified to condition approval of the Joint Application on an assurance or commitment to not integrate and/or remove Huawei equipment from the wireless networks relevant to the proposed transaction. Such a condition will only limit the choice of suppliers available to the Applicants and diminish the prospects for innovation, lower prices, and other benefits of a more highly competitive network equipment market—which is not, we submit, in the public interest.

Huawei respectfully requests that the Commission rely on the facts in its evaluation of the public interest in the Joint Application and reject any condition supposedly intended to mitigation a national security concern with respect to Huawei’s telecommunications network equipment that, in fact, will result in public interest harms and no material benefits.

Sincerely,

/s/ Dennis J. Amari

Dennis J. Amari
Director, Regulatory Affairs
Huawei Technologies, Inc. (USA)

cc: Jacob Lew, Secretary, U.S. Department of Treasury
Eric Holder, Attorney General, U.S. Department of Justice
Janet Napolitano, Secretary, U.S. Department of Homeland Security

²⁶ *Who’s Afraid of Huawei? Security Threats and China’s New World-Beater*, THE ECONOMIST, Aug. 4-10, 2012, at 9.

²⁷ *Id.*

²⁸ *Id.* The article states, “Blocking Huawei...while allowing gear from, say, Alcatel-Lucent or Ericsson on a network may make politicians feel good. But it is no guarantee of security.” *Id.*

²⁹ *Id.*